CorreLog®

WMI Adapter Software

Users Manual

http://www.correlog.com mailto:info@correlog.com

CorreLog, WMI Adapter Users Manual

Copyright © 2008 - 2015, CorreLog, Inc. All rights reserved.

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.

Table of Contents

Section 1: Introduction	……..	5
Section 2: Software Installation	……..	9
Section 3: Software Operation	……..	17
Appendix: Installation Checklist	……..	25
Alphabetical Index	……..	27

Section 1: Introduction

This manual provides a detailed description of the CorreLog WMI Monitor software. This is an optional set of files and executables added to the CorreLog Server order to expand the role of the CorreLog to allow collection of events using WMI protocol. This provides "Agentless" operational capability to the CorreLog server.

The manual provides information on specific features and capabilities of this special software, including installation procedures, operating theory, application notes, and certain features not documented elsewhere.

The WMI Monitor software consists of several components. A background process continuously polls WMI devices for information, and sends alerts to CorreLog (in the form of syslog messages) when certain events match specific patterns. A "Messages > Adapters > WMI" screen is provided to allow the user to configure system logins and match patterns.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog system's role within an enterprise to include WMI agentless monitoring.

Overview Of Operation

The WMI Monitor Adapter software extends the CorreLog system to permit polling of device states using standard WMI. This allows CorreLog to operate in an agentless mode, managing Windows event logs through standards-based WMI facilities and services

The CorreLog WMI background process continuously polls devices for events using WMI. The system pulls down recent events, de-duplicates these events, and compares new events to match patterns. When specific match patterns exist, a syslog message is sent to CorreLog. The event appears in CorreLog in a manner almost identical to events that are sent via the standard Windows Tool Set and Windows Agent.

The CorreLog WMI background process is configured and monitored using a tightly coupled integration with the main CorreLog web interface. The user configures match patterns and user logins via the "Messages > Adapters > WMI" screen.

WMI Agentless Monitoring Basics

Generally, agentless monitoring using WMI is less secure than agent based monitoring, and provides less flexibility and scalability. Additionally, agentless monitoring requires extensive setup and administrative labor to get running.

However, there may be certain situations where agentless monitoring using WMI cannot be avoided. For example, an organization may have specific policies against adding software to systems, but is quite agreeable to creating user profiles to access WMI data. In this case, the CorreLog WMI monitor can provide agentless monitoring, log file collection, and correlation without installing any software whatsoever on a managed Windows platform.

WMI Monitor System Software Components

The CorreLog WMI software comes as a single downloadable package in self-extracting WinZip format. This package is installed at the CorreLog server (as described in detail within Section 2 of this document). The package contains the following specific components.

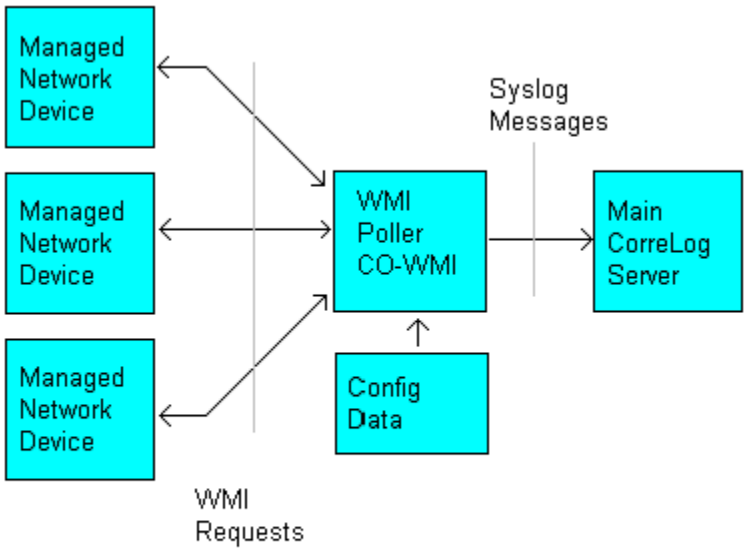
- **CO-WMI.exe Program.** This is the polling agent that is responsible for gathering WMI information on the system. The process is configured to run on CorreLog system startup (via the "System > Schedule" screen, as documented below.)

- **WMI Configuration Screen.** This is a support screen, available under the "Messages > Adapters > WMI" tab of the CorreLog web interface as part of the Windows component installation. This screen allows the user to configure the devices to be polled, as well as the message severities and timeouts for the polling process.

System Block Diagram

The CorreLog WMI Monitor process consists of a single background process, which executes at the CorreLog server. This process reads configuration data that has been configured by the operator, and continuously polls a list of devices and event log combinations, fetching event data from the device and delivering it to the CorreLog server.

As the list of managed devices and event logs is polled for values, the WMI software compares each message to match patterns. When a specific pattern or wildcard is matched, the WMI Poller process issues a Syslog message to the Main CorreLog server. The operator configures the message severity and keywords in a fashion identical to the standard CorreLog Windows Agent program.



As indicated in the above diagram:

1. The CO-WMI.exe process (installed and configured as described in the next chapters) continuously polls a list of managed devices.

2. The polling process is controlled and monitored by configuration data that is configured by the operator using the "Messages > Adapters > WMI" screen of the Main CorreLog Server web interface.

3. When certain WMI events match specific patterns, the CO-WMI.exe program sends syslog messages (of appropriate severity) to CorreLog where they appear in the main "Messages" screen.

The device that was the source of the event appears in the event log as if the device actually sent the message using the Windows agent program.

Supported Platforms

The WMI software can be installed at any existing CorreLog Server site. Both 32-bit and 64-bit platforms are supported (but no benefit is obtained by executing on a 64-bit platform, and a 32-bit platform is generally recommended.)

Note that a special version of CorreLog Server (referred to as the WMI Agentless Collector Server) is available for those customers interested ONLY in collecting the data relaying WMI event logs to another server. This special version is available after consultation with CorreLog Support, and executes on a wide variety of target operating systems, including Windows 200X, Vista, XP, and potentially other platforms. (Contact CorreLog Support for more information.)

As with the main CorreLog Server system, this program does not require .NET, Java, or any other supporting software, hence the program is easily installed on a wide selection of platforms.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install the CorreLog WMI Monitor software. Note that the only required components of the system are the CO-WMI.exe program and the WMI configuration screen, documented herein. Other information on the CorreLog server can be found in the standard "User Manual", including operation and application notes that will be of assistance in processing the WMI messages generated by the CO-WMI.exe program, and received by the CorreLog Syslog receiver process.

Section 2: Software Installation

The CorreLog WMI Monitor software is usually delivered as a self-extracting WinZip file. The installation requires various manual installation steps needed to configure permissions and access to WMI data on managed Windows devices. Basic installation steps are as follows:

1. The user obtains the CorreLog WMI Monitor software, in self-extracting WinZip format, and executes the self-extracting WinZip file. This unzips the WMI software into the CorreLog Windows Distribution, including all configuration data and executables.

2. The user configures the CO-WMI.exe process to start when the main CorreLog Server processes start (via the CorreLog "System > Schedule" screen.) This also requires the user to configure the service to run as "Administrator", with a valid local administrator login for the CorreLog platform.

3. The user configures WMI monitors for the various managed platforms, consisting of IP addresses, event logs, and match patterns. Each device requires a valid login that permits reading of WMI data.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

The WMI Monitor software can be installed on a variety of platforms and operating systems, including Windows 2K, Windows 2008, Windows 7, and Windows Vista operating systems. Prior to installing the WMI Monitor software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

The WMI Monitor software requires no significant disk space or CPU requirements beyond the normal footprint of the CorreLog server. There is generally no extra disk space load due to this software.

To insure proper installation of the program, the user should close all windows, and temporarily disable any port blocking or Virus Scan software on the system. The existing CorreLog server process should be stopped prior to the installation. Reboot, after installation, is not required.

Windows Installation Procedure

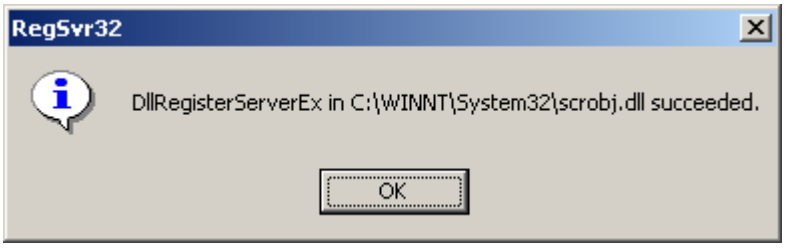
The specific steps needed to install the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Stop the CorreLog Server processes via the Windows Service Manager, or via the "Start and Stop Services" utility found in the Windows Start menu. Verify with the Windows "Task Manager" that all CorreLog processes (i.e. processes beginning with a "CO-" prefix) are stopped.

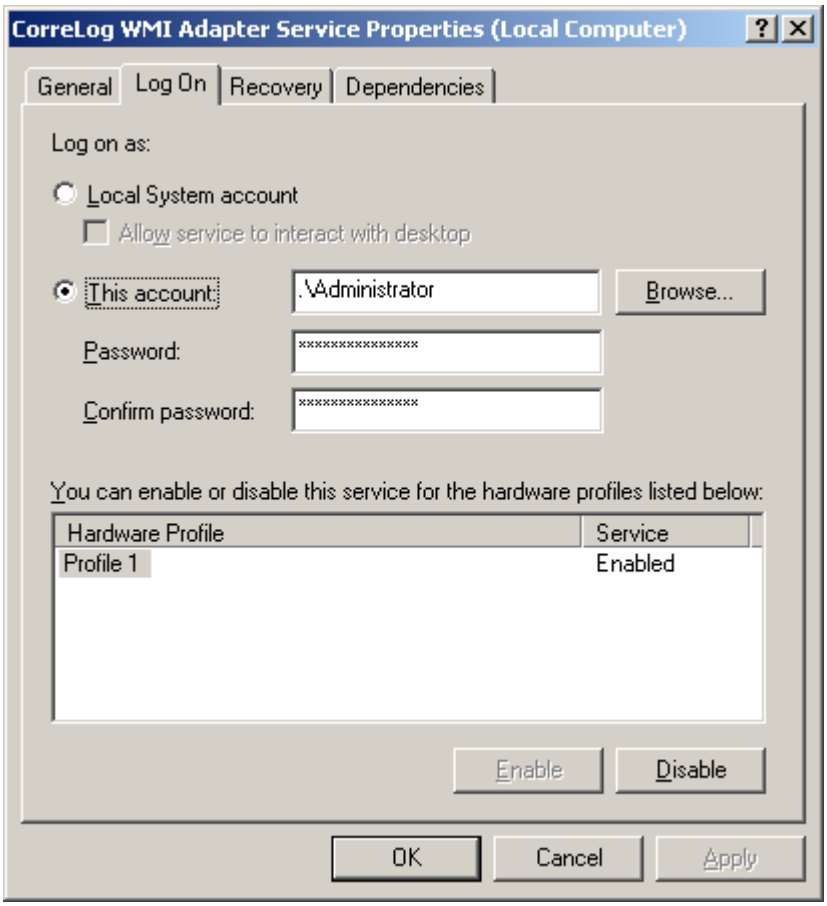
3. Obtain and execute the "co-n-n-n-wmi.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog").

4. After extracting files, change working directories to the "CorreLog\wmi" directory and manually execute the "WMI-INSTALL.exe" file to finish the installation. (This installs the CO-wmi.exe service, and registers other DLL components needed to run the system.) Successful installation results in a dialog being displayed, such as the following:



Comment: On Windows 2008, Windows 7, and Vista systems, the program should be executed with elevated permissions. The operator should launch the program by right-clicking, and selecting "Run As Administrator". Failure of the operator to execute the "WMI-INSTALL.exe" program with elevated permissions may cause the installation procedure to silently fail.

5. After installing the CO-wmi.exe service, access the Windows Service manager and configure the "CorreLog WMI" service with a valid Administrator name and password. An example of the Windows Service Manager screen is showed below.



Comment: If the user skips this step, the WMI monitor will not be able to poll any WMI data. This step can be accomplished any time after installation, if the step is skipped here, but will be required for proper operation of the CorreLog WMI monitor software.

6. Restart CorreLog via the Windows Start menu, or via the Service manager. (Start the "CorreLog Service" framework. The other CorreLog services will be started by this main service.)

7. Log into the CorreLog web interface using a CorreLog "admin" type login, and access the CorreLog scheduler screen, by clicking the "System > Schedule" tabs.

8. On the "Schedule" screen, click "AddNew" to add a new item to the list of scheduled commands.

9. On the "AddNew" screen, select a "Start" directive and enter the following command:

   ```
   CO-WMI.exe –start
   ```

   Comment: This directive will cause the CO-WMI.exe service to automatically start when the CorreLog system first starts. The user can also start the CO-WMI.exe program via the Windows Start menu "Start and Stop Services" utility.).

10. Stop and restart the CorreLog Server processes via the Windows Service manager, or via the "Start and Stop Services" utility.

11. Verify with the Windows "Task Manager" that the "CO-WMI.exe" process is now running on the system.

WMI Software Configuration

The WMI Monitor software requires that managed devices respond to WMI requests from the CorreLog server. This is the normal condition (however some sites may purposely disable WMI responses from devices, and those selected devices will not be manageable by CorreLog.)

Once the CO-WMI.exe program has been installed and is running on the system, the user can configure the list of devices and event logs that are polled by the agent. The user accomplishes this activity via the "Messages > Adapters > WMI" tab of the web browser interface. (The "Adapters" tab is automatically added to your system, if it does not already exist.)

Note that, by default, the CO-WMI.exe program does not poll any devices. The user must configure one or more device IP addresses, which is polled by the CO-WMI.exe program.

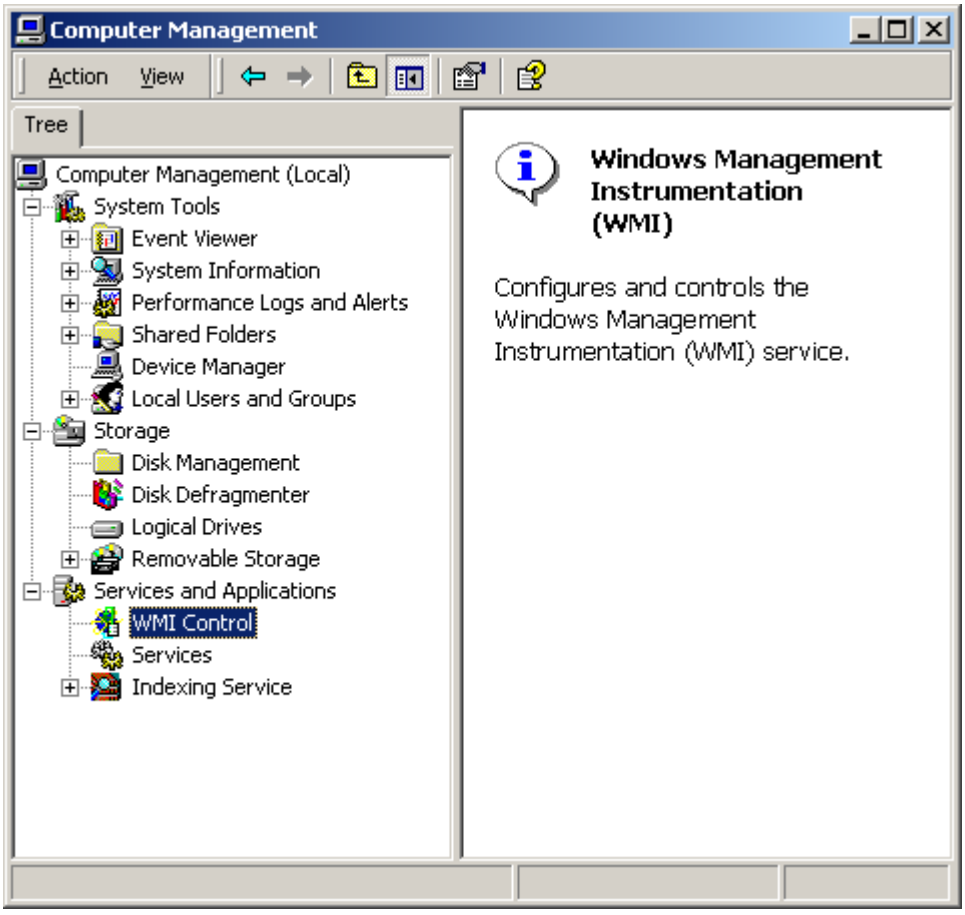
The user clicks on the "AddNew" button to add a new monitor. The user provides the IP address, and the name of the event log to fetch, such as "Security", "Application", "System" or some other name that appears in the Event Viewer. In addition to specifying an IP address and event log, each entry also requires the username and password that permits access to the WMI software. The user can

specify an "Administrative" login and password, or can define a new user that has access only to WMI data.

To allow permissions to the WMI data on a particular platform, the user executes a procedure such as the following.

1. The administrator adds a new user for the system, such as a WMI user, that will be granted permission to the WMI data.

2. The administrator accesses the "Computer Management" dialog for the platform, such as via the Control Panel Administrative tools, clicks on "Services and Applications", and clicks the right-mouse button on the "WMI Control " entry to select "Properties.



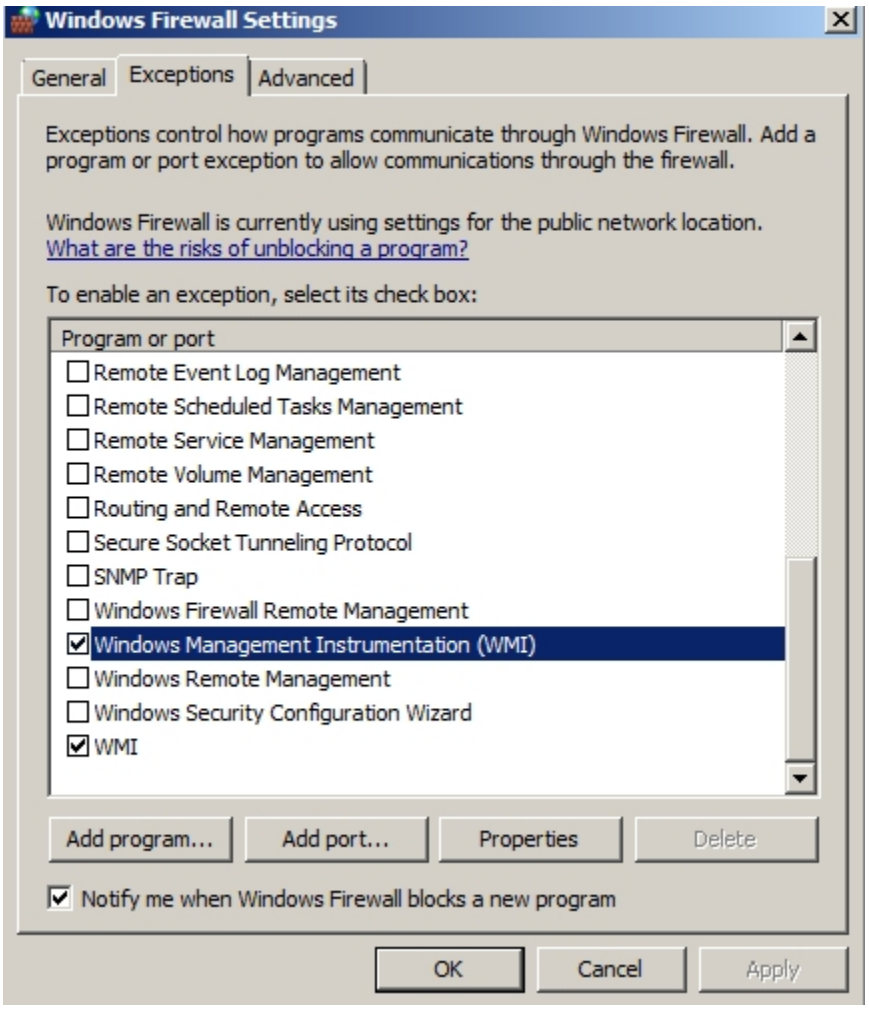
3. On the WMI Control menu, the user clicks the "Security" tab, and then clicks the "Security" button to access the standard security controls to permit the user added in Step 2 to access the WMI data.

Comment: Rather than creating a special WMI user, the administrator can simply

enter an administrative login and password at the CorreLog WMI screen, which will provide access to the WMI data. CorreLog does not store this password in clear text on the system. All stored passwords are securely encrypted via a one-way algorithm Operators may trust the extensive encryption capabilities of correlog and its ability to protect private data.

Firewall Exceptions

On Windows 2008, Windows 7, and Vista systems, the firewall should be modified as part of the standard operational configuration to permit WMI requests. Microsoft provides a specific setting to support WMI, as depicted below. The user should click all "WMI" related entries to be exceptions.



Failure to adjust the WMI firewall settings will result in failures when attempts are made to connect to the WMI interface of these platforms. All devices participating

in the WMI session (including the CorreLog server, if applicable) should permit WMI access, as show above.

Testing the Installation

The user can test the installation, after adding one or more devices, by drilling down on the "Raw Output" hyperlink on the Adapters > WMI screen to see if data is being collected, and to inspect any errors with the system. Common errors with the system are generally attributed to user input errors when specifying a WMI monitor, such as invalid IP address, usernames, etc. Additionally, WMI permissions may be misconfigured for the specified users, and the COM and DCOM software may not be running or supportive of WMI.

The user can test the installation at the command line using the "getevent.exe" program, found in the CorreLog "system" directory. This utility allows the user to get events at a command line prompt. The utility is documented in Section 3 of this manual.

Section Summary, Additional Notes

1. As part of the installation process, the installer must run the "CorreLog/wmi/WMI-INSTALL.exe program This will add the CorreLog WMI Adapter Service" to the system, and register DLLs used by the WMI polling process. Failure to perform this step will cause the WMI polling agent to fail.

2. On Windows 7, Windows 2008 and Vista systems, the user must execute the WMI-INSTALL.exe program using elevated permissions. Right click on a CMD.exe shortcut and select "Run As Administrator". Or, the user can execute the "runas" command to create a command prompt with elevated permissions. Failure to perform this step will cause the WMI-INSTALL.exe program to silently fail to register DLLs and / or install the CO-wmi.exe service.

3. The installer must provide an administrative login for the "CorreLog WMI Adapter" service by drilling down into the Service, clicking the "Log On" tab, and then providing the administrative username and password. Failure to perform this step will cause the WMI polling agent to fail.

4. The Administrator may configure a special user for the WMI software. Or the operator can add the administrative login for each WMI monitor on the system. The easiest way to configure access to the remote WMI interface is to use an Administrative login for each monitor.

5. All Administrative passwords used by the WMI monitor are encrypted using a one-way encryption algorithm. These passwords will not be visible

to any operator, including operators with access to the CorreLog server platform.

6. The "system\GetEvt.exe" command line program can be used to test the WMI library. This program is useful for fetching event logs from a WMI device. The specified device MUST be configured in the CorreLog WMI tab.

Section 3: Software Operation

Once the CorreLog WMI Adapter program is installed, it makes use of reasonable default values. The operator only needs to configure a series of WMI monitors, consisting of an IP address, event log, and username / password parameters for each monitor. Additionally, the user needs to configure match patterns and a default severity for the system:

1. The operator configures one or more IP address and Event Log combinations for the system. These "WMI Monitors" include a username, password, and default facility and severity.

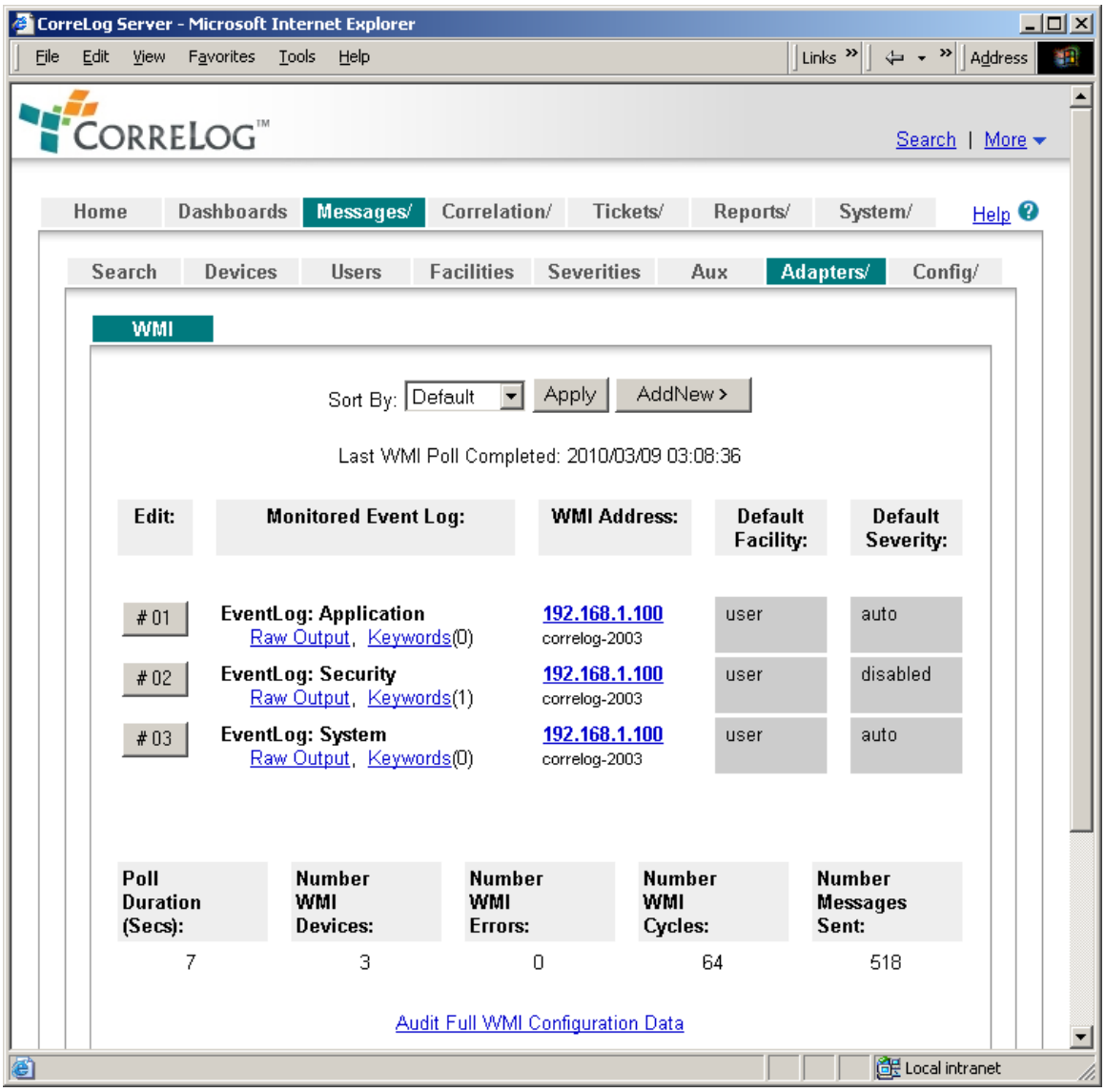
2. The operator configures keywords for each monitor. These are used to filter the message data, and assign severities to messages. The user can select a specific severity for all messages, or can use the special "auto", or "disabled" severity, as discussed herein.

3. The operator can view the raw WMI data obtained on the system (before any keywords are applied) via a special "Raw Output" hyperlink associated with each WMI monitor. This Raw Output can also contain WMI errors, possibly associated with invalid authentication to the WMI data.

This section provides a description of these optional software elements, their usage, and other considerations, including screenshots and explanation of monitor configuration values.

WMI Monitor Screen

As part of the Windows installation, a new tab is created in the "Message > Adapters" section of the CorreLog web interface, which permits the user to configure various parameters associated with the WMI Monitor program. This screen is available only to CorreLog administrators. The screen is depicted below.



The above screen is a standard CorreLog screen, incorporating an "AddNew" button to add new monitors, and "Edit" buttons associated with each WMI monitor.

The WMI Monitor screen provides the following parameters, which are read by the CO-WMI.exe program

- **Monitored Event Log.** Each WMI monitor consists of an event log, and an IP address combination. The event log can be "System", "Security", "Application", or any other name that is listed in the "Event Log Viewer" for the platform.

- **WMI Address.** The IP address parameter specifies a Windows 200X, Vista, or Windows 7 target of the WMI operation. The user must know an Administrative login and password to each managed device (configured via the "AddNew" and "Edit" screens.) Although the remote device may run the CorreLog agent, it is typically the case that no CorreLog agent will execute on the target platform.

- **Default Facility.** This value is the syslog facility for all messages sent by the WMI monitor. A single facility is used for all messages associated with the event log and device. (The user can override this facility, as with any message, via the "Messages > Config > Overrides" tab.

- **Default Severity.** This value is the default syslog severity for messages if no match for a keyword is specified. This can be any standard severity, as well as the special "auto" severity (which automatically assigns a severity based upon the event type) and the special "disabled" severity (which causes no message to be sent unless a keyword specifically matches the message.)

- **Raw Output Hyperlink.** This hyperlink allows the user to inspect the raw output of the last WMI operation for the specified IP address and log combination. The user can view the last 200 messages on the system via this hyperlink. Messages are sorted with earliest messages listed first. This link can also be used to inspect any errors associated with the WMI operation.

- **Keywords Hyperlink.** This hyperlink allows the user to configure keywords that set the severity of the system. Each keyword consists of a simple keyword or wildcard. When a message matches the keyword, then the specified severity is used with the message. In particular, users can disable certain messages, or assign their own precise severities for messages.

Monitor Status Bar

At the bottom of the WMI Monitor screen, beneath the list of WMI Monitors, are a series of metrics that indicate the progress and state of the CO-WMI.exe

background process. These metrics are updated at the end of each poll cycle, and provide the following information:

- **Poll Duration.** This is the time in seconds needed to poll all monitors on the system one time. The time is calculated at the end of each poll cycle, and will indicate the general load on the system. If the time is less than 60 seconds, then the CO-WMI.exe program will wait until at least 60 seconds have elapsed before resuming polling. (See additional notes below.)

- **Number Of WMI Devices.** This is the total number of devices polled during the last cycle. It represents the total number of WMI requests that have been issued by the program during the last poll cycle. This number will be equal to the number of WMI Monitors multiplied by the total number of devices for each monitor. The value will be under 10,000.

- **Number Of WMI Errors.** This is the total number of errors during the last cycle. This typically indicates that there is an internal permission problem within CorreLog, or that the installation is corrupt. The WMI software does not increment this field if the device is offline, or if a DCOM type error exists.

- **Number Of WMI Cycles**. This is the total number of poll cycles since the system started. This value increments each time a complete poll cycle finishes. This value, when divided by the system up time of the CorreLog server, will indicate the average time to poll all WMI Monitor devices and objects.

- **Number of Messages Sent.** This is the total number of Syslog messages that have been issued by the WMI polling process to the CorreLog server since the system started, useful for assessing how busy the polling monitor is.

Creating Threads, Tickets, and Alerts

The messages sent by the WMI Monitor are almost identical to the messages sent by the CorreLog Windows Agent. The only major difference is that each WMI message contains a special "WMI Time:" field appended to the message, which is a unique identifier of the local time of the managed device. This field can be used to correlate the WMI monitor messages in a slightly different way, depending upon the requirements of the user.

The basic method for correlating the WMI Monitor messages is no different that the techniques discussed elsewhere. The basic steps are provided below.

1. The operator creates a thread to tabulate the messages sent by the monitor using the "Correlation > Threads > Add New" screen. This screen

is used to collect all the messages of a particular type (such as all messages with "WMI" in their content.)

2. The operator creates an Alert for the thread counter using the "Alerts > Counters> Add New" screen. This alert will send a Syslog message back to the main list of messages when one or more messages are received during an interval of time. As is always the case, when an alert is triggered, a single message is sent back to CorreLog, and a single ticket is opened while the alert is set. (See additional notes below.)

3. The operator optionally identifies an "Assignee" for the alert via the "Alerts > Counters > Add New" screen. This causes a ticket to be opened on the system, and assigned to a particular user or a ticket group. The user can assign a ticket to any existing user, or ticket group.

4. The operator optionally adds a "Ticket Action" to the system, which sends e-mail (or performs some other action) when a new ticket is opened on the system, providing a real-time indication that a timeout threshold of the WMI Monitor software has been violated. This message will typically contain the descriptive text entered by the operator when the alert was created, which may be slightly (or totally) different than the originating WMI Monitor message.

As a special note, if only one ticket is to be opened on the system per WMI threshold violation (as will often be the case), then the "Alert Interval", configured on the "Alerts > Counters" screen, should be higher than the "Poll Interval" displayed at the lower left of the "Messages > Adapters > WMI" screen. Additionally, the "Auto-Learn" function for the alert should probably be disabled to prevent this interval from changing automatically.

Failure to understand or implement this consideration may result in multiple tickets being opened for the same system threshold violation, which will not be desirable, especially if one of the ticket actions is to send e-mail or provide other intrusive notifications to the ticket assignee.

The "Getevent.exe" Utility

As part of the WMI installation, CorreLog provides the "getevent.exe" program in the "system" directory. This program is useful for testing and debugging the WMI system, as well as acquiring data from remote Windows platforms via WMI protocol (such as for use with the CorreLog "import" facility.)

The "getevent.exe" program requires an Administrative login to execute. If the user is not an administrator, the program will fail with one or more possible error messages (depending upon the user's configuration and permissions.)

To execute the "getevent.exe" program, create a cmd.exe prompt (possibly with elevated Administrative permissions on Windows 7 or Vista.) Then change working directories to the CorreLog "system" directory, and execute the program as follows:

```
Getevent.exe (ipaddr) (logname) [ -all | -raw ]
```

(ipaddr)

This is the IP address of a WMI device configured on the WMI screen of the CorreLog system, in standard N.N.N.N format.

(logname)

This is the Log name of a WMI device configured on the WMI screen, such as "Security", "Application", "System", etc. The value is not case-sensitive

(options)

If no option is specified, the utility lists last 200 lines of the specified event log in standard CorreLog "import" format. Other valid options are "-all" to list all the messages, and "-raw" to list the raw WMI list output.

Note that the user does not specify a username or password as part of the command line invocation. These values are fetched from the CorreLog WMI configuration data based upon the specified IP address and log. This implies that a device cannot be queried unless it has been configured in the CorreLog web interface.

The output is in a format that can be imported into CorreLog. Note that the most recent lines are listed first.

Special Considerations and Caveats

The WMI monitor gathers the last 200 messages from the WMI device, and then compares this to the previous list of 200 messages to see whether any new messages have occurred. This limitation necessarily implies that only the last 200 messages of any event log are reported, and that if more than 200 messages are received during a poll interval, only the most recent messages are reported.

For this reason, the WMI monitor works best when the user has carefully targeted the auditing of the system, configured policies so that only pertinent events are logged. For example, if the target WMI device is extremely busy and has full auditing, it is quite possible that more than 200 messages per minute are logged, and certain messages will be dropped.

Under the direction of CorreLog support, it is possible to expand this 200-message limit to 1000 messages per cycle or higher (via changes to the CorreLog configuration and executable.) This may degrade overall performance of the system, since 1000 messages are necessarily fetched each poll cycle regardless of whether any new messages have been logged. However, at some sights this may be tolerable and desirable.

Section Summary, Additional Notes

1. The CO-WMI.exe program polls each device group entry no faster than once per minute.

2. The user can determine the poll time and response time for the CO-WMI.exe program by drilling down into the WMI Monitor name hyperlink, which shows the current response time values for all devices during the last poll cycle.

3. Caution should be taken to avoid specifying devices in the poll lists that do not support WMI. This can substantially degrade the performance of the polling (especially if the timeout and retry value is high for the monitor.

4. The "Poll Interval" metric, available at the bottom-left of the WMI Monitor screen, indicates the time (in seconds) needed to poll all values during a single cycle. This value, if over 60 seconds, indicates the typical duration between poll cycles, and the rate at which the WMI Monitor will send Syslog messages when a threshold is violated.

5. The maximum number of messages polled per cycle from any WMI box is 200 messages. If the remote device logs more than 200 messages since it was last polled, the WMI monitor will fetch only the 200 most recent messages during that poll cycle. This value can be changed by CorreLog support and professional services, if needed.

6. When configuring a CorreLog alert, the "Alert Interval" should be greater than the "Poll Interval" value to prevent multiple tickets from being opened for a single incident. Additionally the "Auto-Learn" function for the alert should typically be disabled.

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Appendix: Installation Checklist

Item	Description	OK
1	The CorreLog "WMI-INSTALL.exe" program has been executed with no errors. (This program is found in the "wmi" directory of the CorreLog distribution, and must be run as administrator.)	
2	The "CorreLog WMI Adapter Service" has been installed. (The service is installed via the WMI-INSTALL.exe program, above.)	
3	The "CorreLog WMI Adapter Service" has been modified to run as "Administrator", and service password has been configured for the service. (The service password is configured via the "Log On" tab of the "Service Properties" tab.)	
4	The CorreLog "System > Schedule" has been modified to include the CO-WMI.exe -start" directive. (This causes the service to start when CorreLog starts.)	
5	After restarting the CorreLog system, CO-wmi.exe program is running in the task manager. (The process is started when CorreLog starts, and is under the control of the Windows Service Manager. If the service fails to start, verify that the logon information, configured in step 3 above, is correct.)	
6	Each target computer WMI interface has been enabled and configured via the "Computer Management > Services and Applications > WMI Control > Properties" Windows dialog. (The WMI services must be running on the target platform.)	
7	One or more devices and event logs have been added to the "Messages > Adapters > WMI" tab of the system.	
8	The "Default Severity" of the event log, added above, is other than "disabled", or at least one keyword has been added to the keyword list of the event log.	
9	The "Raw" link of the system indicates that messages are being fetched for the target event log.	

Alphabetical Index

A

Action / 21
Adapter / 6 15 17 25
Adapters / 5 6 7 8 12 15 18 21
Addnew / 12 18 19
Address / 19
Administrative / 9 12 13 15 19 21 22
Administrator / 9 10 11 15
Agentless / 5 6
Agentless, WMI Monitoring Basics / 6
Alert / 21 23
Application / 12 19 22
Applications / 13
Assignee / 21
Auto-learn / 21 23

B

Basics, WMI Agentless Monitoring / 6
Block, System Diagram / 7

C

Caution / 23
Caveats / 22

Cmdexe / 15
Co-wmiexe / 6 7 8 9 11 12 15 19 20 23
Comment / 11 12 13
Common / 15
Components / 6
Components, WMI Monitor System Software / 6
Computer / 13
Config / 19
Configuration / 7 12
Configuration, WMI Software / 12
Considerations / 22
Correlation / 20 21
Creating / 20
Cycles / 20

D

Dcom / 15 20
Default / 19
Devices / 20
Diagram / 7
Diagram, System Block / 7
Disk / 10
Distribution / 9
Dlls / 15
Duration / 20

E

Errors / 20
Event / 12 17 19
Exceptions / 14
Exceptions, Firewall / 14
Existing / 10

F

Facility / 19
Failure / 11 14 15 21
Firewall / 10 14
Firewall Exceptions / 14

G

Geteventexe / 21 22

H

How To Use This Manual / 8
Hyperlink / 19

I

Installation / 9 10 15
Installation, Software / 9
Installation, Windows Procedure / 10
Installexe / 11 15
Interval / 21 23
Introduction / 5 5

K

Keywords / 19

M

Management / 13
Manager / 10 11 12
Manual / 8 10
Manual, How To Use This / 8
Messages / 5 6 7 8 12 19 20 21
Monitor Status Bar / 19
Monitored / 19
Monitoring / 6
Monitoring, WMI Agentless Basics / 6
Monitors / 17 19 20

N

Nnnn / 22
Notes / 15 23
Number / 20

O

Operation / 6 17
Operation, Software / 17
Operators / 14
Output / 15 17 19
Overrides / 19
Overview / 6

P

Page / 25
Poll / 20 21 23
Poller / 7
Procedure / 10
Procedure, Windows Installation / 10
Program / 6
Properties / 13

R

Reference / 10
Requirements / 10
Restart / 12
Right / 15

S

Schedule / 6 9 12
Security / 12 13 19 22
Sent / 20
Server / 5 8 9 10 12
Service / 10 11 12 15
Services / 10 12 13
Severity / 19
Software / 6 9 12 17
Software, WMI Configuration / 12
Software, WMI Monitor System Components / 6
Software Installation / 9
Software Operation / 17
Space / 10
Start / 10 12
Status / 19
Status, Monitor Bar / 19
Step / 13
Summary / 15 23
Syslog / 7 8 20 21 23
System / 6 7 9 12 19 22
System, WMI Monitor Software Components / 6
System Block Diagram / 7

T

Task / 10 12
Testing / 15

Threads / 20
Ticket / 21
Tickets / 20
Time / 20
Tool / 6

U

Under / 23
User / 8 10
Utility / 21

V

Verify / 10 12
Viewer / 12 19
Virus / 10
Vista / 10 11 14 15 19

W

WMI Agentless Monitoring Basics / 6
WMI Monitor System Software Components / 6
WMI Software Configuration / 12
Windows / 6 7 8 9 10 11 12 14 15 18 19 20 21 22
Windows Installation Procedure / 10
Winzip / 6 9
Wmiexe / 12 23